IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re: Clearview AI, Inc. Consumer Privacy Litigation	)	Case No. 1:21-cv-00135
	)	Hon. Sharon Johnson Coleman

BRIEF OF AMICI THE FIRST AMENDMENT CLINIC AT DUKE LAW AND PROFESSORS OF LAW JANE BAMBAUER AND EUGENE VOLOKH IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

STATEMENT OF INTEREST

Professors of Law Jane Bambauer, of the University of Arizona, and Eugene Volokh, of the University of California Los Angeles, and the First Amendment Clinic at Duke Law School, frequently engage in research, legal representations, and scholarship pertaining to the intersection of the First Amendment and privacy law. Collectively, amici have authored numerous amicus briefs and articles concerning free speech issues and have a wealth of expertise and knowledge relating to matters relevant to this case.

Amici write to assist the court in its analysis of the application of Illinois' Biometric Information Privacy Act (BIPA), 740 ILCS § 14 (2008), to faceprints derived from publicly accessible photographs. Amici contend that the application of BIPA to the creation of such faceprints, by Clearview AI ("Clearview") or any other person, is unconstitutional. The First Amendment protection of free speech applies equally to regulations that target the "upstream" speech-creation activities—such as information gathering and analysis—that make informed expression possible as it does to the resulting expression. Here, BIPA's restriction on the creation of new information derived from publicly available information undermines free speech principles by purposefully halting the production of speech and knowledge. Moreover, because BIPA is not tailored to an articulable and cognizable privacy harm, it violates the First Amendment.

ARGUMENT

I. The First Amendment Protects the Collection and Analysis of Publicly Available Information.

The "freedom of speech" protected by the First Amendment is an expansively defined right; it includes not just the end products of speech, such as expression and communication, but also the preceding or "upstream" activities that make that expression possible. *See Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011) ("[T]he creation and dissemination of information are

speech within the meaning of First Amendment."); *Citizens United v. Fed. Election Comm'n*, 588 U.S. 310, 336 (2010) ("[L]aws enacted to control or suppress speech may operate at different points in the speech process."). This is logical, as activities such as information gathering, research, recording, and analysis are bedrock processes of speech creation.

Courts have repeatedly protected the activities of gathering and using public information in a variety of contexts, including by guaranteeing access to courts and public hearings and the right to record the actions of public officials. *See, e.g.*, *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 604 (1982) (protecting public access to criminal trials); *Bd. of Educ. v. Pico*, 457 U.S. 853, 867 (1982) (plurality opinion) (protecting public access to libraries, because "the right to receive ideas is a necessary predicate to the recipient's meaningful exercise of his own rights of speech, press, and political freedom"); *Richmond Newspapers v. Virginia*, 448 U.S. 555, 576 (1980) (plurality opinion) (protecting public access to courtrooms, because "[f]ree speech carries with it some freedom to listen ... '[w]ithout some protection for seeking out the news, freedom of the press could be eviscerated'"); *Pochoda v. Arpaio*, 2009 WL 1407543, at *4 (D. Ariz. 2009) (protecting "observation of [a] demonstration" in a public forum, because the "the right to hear" is "no less protected" than "the right to speak,"); *Goldschmidt v. Coco*, 413 F. Supp. 2d 949, 952–53 (N.D. Ill. 2006) (protecting note-taking in courtrooms, because it allows observers to "revisit what they have heard or read," and thus to "more fully and accurately evaluate and communicate the subject matter"); *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 903–904, 907 (1982) (protecting public surveillance by individuals enforcing a boycott).

The expansive protection for the activities that precede expression serves important First Amendment values because each step in the production of speech—from information gathering to analysis to creation to dissemination—is critical to ensuring a healthy marketplace of ideas. As James Madison recognized, both knowledge and the gathering of knowledge are crucial for

maintaining an informed electorate and thus an effective democracy. *See* 9 WRITINGS OF JAMES MADISON 103 (Hunt ed. 1910) ("A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."). When the law prevents the public from gathering and analyzing information, and creating new information from it, the law deprives society of the opportunity to learn about, discuss, and form new opinions. To function, the marketplace of ideas depends on a myriad of uncoordinated insights and information, and the government's purposeful interference with that process must be viewed with skepticism.

II. The Speech/Conduct Distinction Is Easy to Apply When a Law Purposefully Targets Information Gathering, Analysis, and Creation.

BIPA, as applied to the creation of faceprints, is a speech restriction because information gathering, analysis, and creation are protected by the First Amendment. In other contexts, courts have had to draw difficult lines between speech and conduct when a law punished conduct with significant expressive value. *See, e.g.*, *United States v. O'Brien*, 391 U.S. 367, 376 (1968) (burning of draft cards). However, the speech/conduct distinction is not relevant when the government interferes with the speech creation process for the purpose of disrupting the creation of new information. Protecting the creative process is tantamount to protecting the end product; the speech right is meaningless without protection for the production of that speech. *Cf. Desnick v. American Broadcasting Cos.*, 44 F.3d 1345, 1355 (7th Cir. 1995) (holding that both the "broadcast" and the "production of the broadcast" were protected by the First Amendment); *Anderson v. Hermosa Beach*, 621 F.3d 1051, 1061–62 (9th Cir. 2010) ("[N]either the Supreme Court nor our court has ever drawn a distinction between the process of creating a form of pure speech . . . and the product of these processes . . . in terms of the First Amendment protection afforded.").

As circuit courts around the country have recognized, the right to gather and use non-private information is inextricably intertwined with the right to produce the speech upon which that information is based. *See e.g., Fields v. Philadelphia*, 862 F.3d 353, 358 (3d Cir. 2017) ("The First Amendment protects actual photos, videos, and recordings and for this protection to have meaning the Amendment must also protect the act of creating that material. There is no practical difference between allowing police to prevent people from taking recordings and actually banning the possession or distribution of them.") (internal citation omitted); *ACLU v. Alvarez*, 679 F.3d 583, 596 (7th Cir. 2012) ("[T]here is no fixed First Amendment line between the act of creating speech and the speech itself.").

For example, in the Seventh Circuit the public has a clearly established right to make audiovisual recordings in public. *Alvarez*, 679 F.3d at, 595–96. In *Alvarez*, the Seventh Circuit refused to apply Illinois' all-party consent wiretap statute against people who sought to monitor police conduct by recording the police officers' performance of their official duties. *Id.* The statute's requirement of all-party consent burdened individual speech and press rights by restricting the creation of information "at the front end of the speech process." *Id.* at 596. Such a restriction on information gathering "suppresses speech just as effectively as restricting the dissemination of the resulting recording." *Id.*

The use of mechanical means such as a camera or computer does not negate First Amendment protection for information gathering. Prohibitions on the use of mechanical devices serve only to "limit[] the information that might later be published or broadcast" and thus burden free speech rights. *Id.* at 596–97; see also *Fields*, 862 F.3d at 359 (noting that recording allows observers to corroborate information and thus see and hear more accurately and facilitates distribution and discussion). Other circuits have protected the right to record in public using similar reasoning. *See, e.g.*, *Animal Legal Def. Fund v. Wasden*, 878 F.3d 1184, 1203 (9th Cir. 2018)

("[A]udiovisual recordings are protected by the First Amendment."); *Turner v. Lieutenant Driver*, 848 F.3d 678, 688–89 (5th Cir. 2017) (First Amendment right to record law enforcement in public); *Gericke v. Begin*, 753 F.3d 1, 7 (1st Cir. 2014) (same); *Smith v. Cumming*, 212 F.3d 1332, 1333 (11th Cir. 2000) (same); *Fordyce v. Seattle*, 55 F.3d 436, 439 (9th Cir. 1995) (same).

The First Amendment also applies when the state burdens the creation of speech by prohibiting or limiting the collection and use of specific types of research data. *See, e.g.*, *West. Watersheds Project v. Michael*, 869 F.3d 1189, 1192 (10th Cir. 2017) (noting that the statutes at issue "target the 'creation' of speech by imposing heightened penalties on those who collect resource data."); *PETA v. Stein*, 2020 WL 3130158, at *9 (M.D.N.C. June 12, 2020) (holding that the government cannot avoid First Amendment analysis by regulating the collection and use of data rather than publication); *Animal Legal Def. Fund v. Otter*, 44 F. Supp. 3d 1009, 1023 (D. Idaho 2014) (holding that unauthorized audiovisual recording qualifies as speech creation and is subject to First Amendment protections); *Sandvig v. Sessions*, 315 F. Supp. 3d 1, 8–9, 15–16 (D.D.C. 2018) (noting that "the First Amendment . . . prohibit[s] the government from limiting the stock of information from which members of the public may draw") (citing *First Nat. Bank of Boston v. Bellotti*, 435 U.S. 765, 783 (1978)). Neighboring jurisdictions have used strict scrutiny to analyze content-based prohibitions that target the collection of specific types of information. For example, in *PETA v. Stein*, the court found that a statute that prohibited the recording and capturing of employer records in a manner that violated an employee's duty of loyalty to his employer violated the First Amendment. *PETA*, 2020 WL 3130158, at *5, *14, *25.

Here, BIPA implicates Clearview's First Amendment rights by limiting Clearview's ability to analyze publicly available photographs and create new information. Faceprints help Clearview "see and hear more accurately" by mechanically improving a process that human minds do naturally—recognizing that a person in one photograph is probably the same person in another.

Fields, 862 F.3d at 359. Using machine learning, Clearview analyzes the publicly available images it has collected and produces faceprints. The process of analyzing and creating a faceprint is equivalent to the creative processes that unavoidably precede expressive activity. *See Anderson v. Hermosa Beach*, 621 F.3d 1051, 1062 (9th Cir. 2010) ("The process of expression through a medium has never been thought so distinct from the expression itself that we could disaggregate Picasso from his brushes and canvas, or that we could value Beethoven without the benefit of strings and woodwinds.").

Finally, Clearview's information gathering and analysis ultimately results in expressive activity. Using its database of faceprints, Clearview runs searches that compare photographs and find matching faces. Clearview then disseminates the results of its searches by sending them to clients. Other firms create faceprints for other purposes like auto-tagging photographs or automatically organizing them into photo albums. Like regulation of a painting process or a writing method, restriction on the creation of faceprints restricts speech by preventing Clearview from making new information. Illinois cannot circumvent the First Amendment by having its restrictions act earlier in the speech process. Restricting speech is just as nefarious at the information gathering and creation stages as at the publication stage.

Amicus ACLU attempts to characterize the creation of faceprints as conduct by using foreboding verbs like "capturing" and "extracting" to describe the information creation process. (Brief of Amicus Curiae ACLU at 4 ("*Capturing* an individual's faceprint is conduct, not speech"), 7 ("BIPA's notice-and-consent requirement is. . . a regulation of the *capture* of a wholly new category of information"); 8 ("the product of additional conduct performed to *extract* private information") (emphasis added). But "capturing" a faceprint from a photograph is no different, in terms of First Amendment analysis, from "capturing" a photograph from a live face. After all, when Henri Cartier-Bresson took the photograph at the root of the controversy in *Gill v. Hearst*

Publishing Co., 40 Cal. 2d 224, 228 (1953) did he not *capture* the young couple in some sense that would have been strange and threatening at the time due to the relatively infrequent use of cameras in public?

ACLU's attempt to distinguish search engines is also unpersuasive. The process of producing faceprints is similar to the process that Google and other search engines use to crawl websites and create a search engine index—a critical component for search.[1] ACLU implicitly concedes that a restriction on the critical components of a text-based search engine would trigger First Amendment scrutiny. (Brief of Amicus Curiae ACLU at 5.) A search engine index collects, organizes, and analyzes names and other identifying features of individuals that allow disparate pieces of information spread across the Internet to be efficiently aggregated. The mechanical aggregation of information by name has privacy implications[2], but the creation of information that facilitates the search of the public web is still protected. ACLU fails to provide a principled distinction between text-based data created in the course of running a search engine and faceprints, which are a graphical equivalent derived from photographs.

Ultimately, restrictions on the creation of faceprints must strike a balance between the strong First Amendment interests in creating new knowledge and countervailing interests in privacy. As with other privacy laws, that balance is struck within First Amendment scrutiny.

III. The Appropriate Standard of Review in This Case Is Strict Scrutiny.

BIPA is a facially content-based restriction on the speech-creation process, and thus on speech, and therefore is subject to strict scrutiny. *Reed v. Town of Gilbert*, 576 U.S. 155, 165 (2015). BIPA explicitly places restrictions on the collection or creation of some categories of

[1] Google Search, *How Google Search Works*, https://www.google.com/search/howsearchworks (last visited July 23, 2021).

[2] Jeffrey Rosen, *Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012) (critiquing the European Right to Be Forgotten and concluding it is incompatible with American First Amendment law).

personal information ("biometric identifiers") and not others (writing samples, photographs, tattoo descriptions, etc.) 740 ILCS 14/10. Clearview can produce sketches of individuals, or faceprints of cats, without implicating BIPA. Thus, the restriction turns on the content of the information—whether it is one of a select set of graphic maps of a human body. *See Barr v. American Ass'n of Political Consultants*, 140 S. Ct. 2335, 2346 (2020) ("A robocall that says, 'Please pay your government debt' is legal. A robocall that says, 'Please donate to our political campaign' is illegal. That is about as content-based as it gets."). Accordingly, under *Reed*, strict scrutiny is presumptively required.

There are no justifications for applying a lower level of scrutiny. Intermediate scrutiny is inappropriate because the creation of faceprints is protected speech that is not a matter of purely private concern. *See Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 759 (1985) (applying a lower constitutional standard in defamation involving matters of purely private concern). Indeed, the recipients of Clearview's information are police departments who engage Clearview's services to pursue their public duty in the investigation of unsolved crimes and the enforcement of criminal laws. The public has an obvious interest in the prompt and accurate identification of criminal suspects. *See* Ronan Farrow, *An Air Force Combat Veteran Breached the Senate*, NEW YORKER (Jan. 8, 2021). Given that the precise name of a rape victim was presumed to be a "matter of public significance" in *Florida Star*, the identity of a suspect or perpetrator should qualify as well. *Florida Star v. B.J.F.* 491 U.S. 524, 536 (1989).

Nor can faceprints be characterized as commercial speech. Speech is given less protection if it does no more than propose a commercial transaction. *Bolger v. Youngs Drug Products Corp.*, 463 U.S. 60, 65–66 (1983). The factors identified in *Bolger* include three characteristics which, in combination, support a conclusion that the document at issue constitutes commercial speech, including: (i) its advertising format, (ii) its reference to a specific product, and (iii) the underlying

economic motive of the speaker. The only factor relevant to Clearview is the third, and that factor could apply equally well to the *New York Times* or any book publisher. A financial interest does not alone convert fully protected speech into lesser protected commercial speech. *See IMDb.com, Inc. v. Becerra*, 2018 WL 979031, at *1 (N.D. Cal. Feb. 20, 2018), *aff'd*, 962 F.3d 1111 (9th Cir. 2020) (finding that IMDb's financial interest in IMDb.com did not transform its web content into commercial speech); *Dex Media West, Inc. v. Seattle*, 696 F.3d 952, 957 (9th Cir. 2012) (finding that the Yellow Pages are not commercial speech).

In any case, BIPA as applied to faceprints derived from publicly available photographs would not satisfy even intermediate review because the privacy interest raised by comparing two publicly available images of faces is not sufficient to meet the heightened scrutiny of requirements of the *Central Hudson* test. *See Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 566 (1980).

IV. BIPA Is Not Well-Tailored to a Specific Privacy Interest, Failing Intermediate and Strict Scrutiny.

BIPA's restrictions on the creation of faceprints from publicly available information violates the First Amendment. In the United States, privacy laws cannot ban the collection, analysis, or subsequent disclosure of information that is already in public view without conflicting with the First Amendment. *Florida Star*, 491 U.S. at 534. This logic carries over to information available on the public Internet. *Sandvig*, 315 F. Supp. at 8–9, 11–12.

The government may be able to set some limits on the creation of faceprints, just as it can set limits on photography, wiretapping, and nonconsensual DNA sequencing that invades a person's seclusion. For some historically and universally recognized zones of privacy, like privacy in the home or in non-public communications, the interests in legal protection may be so strong that free speech analysis is inapplicable or unnecessary. *See, e.g.*, *Bartnicki v. Vopper*, 532 U.S.

514, 533–35 (2001) (noting that privacy interests justify restrictions on collection methods like illegal wiretapping of private conversations). But generally speaking, government impositions on the creation of new information are a direct burden on speech, not an incidental one.

The balance between free speech and privacy is struck by drawing a clear distinction between the collection of public information versus private or sensitive information (e.g., a private conversation or information that, by its very nature, is particularly sensitive such as medical and financial records). Wiretapping and other illicit collection methods implicate privacy interests because they capture the conversations of individuals who are unaware that their conversations and actions are being monitored. *See ACLU v. Alvarez*, 679 F.3d 583, 605 (7th Cir. 2012) (noting that the surreptitious collection of private communications "by way of trespass or nontrespassory wiretapping or use of an electronic listening device clearly implicates recognized privacy expectations."). But unless personal information is unusually sensitive or was learned through a special relationship, people generally are free to say whatever they want about others without the other person's cooperation or consent. *See generally* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049 (2000); Jane Bambauer, *The Relationships Between Speech and Conduct*, 49 U.C. DAVIS L. REV. 1941, 1947 (2016).

Here, Clearview is not violating reasonable expectations of privacy because it built its database of faceprints from photographs that were publicly available on the Internet. Because of the public nature of these photos, users do not have a reasonable expectation of privacy in their content, including their distinctive facial features. While a person may have narrow interests in preventing the analysis of specific, highly sensitive information (such as a DNA sequence or banking password), no individual has a general right to control the inferences and analyses that others make about them based on publicly available information. Since BIPA restricts the

collection or creation of information—visible facial geometry—that is not sensitive, there are no countervailing privacy interests that favor BIPA's application to Clearview.

a. State Interests in Privacy Must Be Specific

First Amendment principles and precedents restrict the government from enacting statutes that create expansive rights of control over information. To avoid conflict with the First Amendment, privacy laws must be narrowly crafted and interpreted to apply to particular contexts where the risks of informational injury outweigh the benefits of free speech. This is true even when intermediate scrutiny applies. The Tenth Circuit, for example, has explained that the government cannot satisfy the substantial interest prong of the *Central Hudson* test by "merely asserting a broad interest in privacy. It must specify the particular notion of privacy and the interest served." *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1234–35 (10th Cir. 1999). In other words, privacy interests are not "substantial" unless the government specifically articulates the interest and properly justifies it. *Id.*

In general, privacy statutes are compatible with the First Amendment *only* if they narrowly target a particular risk to personal information. Valid privacy laws come in two overlapping categories. Some place restrictions on sensitive non-public information such as financial and health data. *See Trans Union Corp. v. FTC*, 245 F.3d 809, 815 (D.C. Cir. 2001) (financial information); *Boelter v. Hearst Communs., Inc.*, 192 F. Supp. 3d 427, 447–48 (S.D.N.Y. 2016) (magazine subscriber lists); *Boelter v. Advance Magazine Publishers*, 210 F. Supp. 3d 579, 602 (S.D.N.Y. 2016) (personal reading information). Others tether restrictions to specific professional or business relationships that produce large quantities of (often sensitive) personal data that are not otherwise publicly available. *See, e.g., National Cable & Telecommunications Ass'n v. FCC*, 555 F.3d 996, 997, 1000 (D.C. Cir. 2009) (telecommunications providers); *Individual Reference Services Group, Inc. v. FTC*, 145 F. Supp. 2d 6, 41–42 (D.D.C. 2001) (financial institutions).

Because BIPA prohibits all individuals from creating faceprints from publicly available photographs, it has an unconstitutionally broad reach that extends well beyond the set of circumstances in which biometric identifiers could be regulated. As applied to Clearview, BIPA seriously burdens the collection and analysis of information that is already available to the public without a sufficiently important reason.

b. BIPA Sweeps Much Further Than a State Interest in Data Security

Data security was one of the motivations for the passage of the Illinois BIPA. *See* 740 ILCS 14/5(a)-(e). If the scope of the act were tailored to the set of biometric information that a bank or employer might reasonably use as credentials to permit secure access to a private account, the law would be narrowly tailored to that anti-hacking purpose. However, BIPA restricts the collection or creation of a significant amount of information that cannot responsibly be used for authentication purposes, including faceprints from publicly available photographs. *See Patel v. Facebook*, 932 F.3d 1264, 1273 (9th Cir. 2019) (primarily describing faceprints as a means to obtain "information that is 'detailed, encyclopedic, and effortlessly compiled'"). Security that can be circumvented using a simple graph of a publicly available photograph of the target is scarcely security at all.[3] Thus, just as an anti-hacking law would be overinclusive if it restricted the collection or dissemination of publicly available photographs, a biometric security law is overinclusive if it restricts the creation of faceprints.

c. There Is No State Interest in Facial Anonymity

If Illinois law had prohibited the comparison of faces *by any means,* including when a human being looks at two pictures and decides whether they are the same person or not, the

[3] Faceprints generated from still photographs do not serve a data security function because anybody with a photograph would be able to break into their target's accounts. *See* Meg Graham, *Illinois Biometrics Lawsuits May Help Define Rules for Facebook,* CHICAGO TRIBUNE (Jan. 17, 2017) (describing how biometric authentication using faces requires "liveness detection" in order to serve a security function.)

impingement on freedom of thought and expression would be obvious. BIPA does not, of course, forbid a person from making a mental map of a person's face, nor does BIPA prohibit the taking of a photograph. It applies only to technologically-assisted recognition of faces. But, because courts have consistently determined that faceprints derived from photographs are biometric information covered by the Illinois BIPA, the law effectively prohibits comparing photographs by using computers.

By seeking to hold Clearview liable for damages, Plaintiffs are attempting to quash an emerging technology based on its efficacy, but the mechanical nature of Clearview's speech creation does not diminish its constitutional protection. The "basic principles" of the First Amendment "do not vary when a new and different medium for communication appears." *Brown v. Entm't Merchs. Ass'n*, 564 U.S. 786, 790 (2011). Similarly, the efficiencies afforded by computers and machine learning do not change the rules of First Amendment scrutiny. *Reno v. ACLU*, 521 U.S. 844, 876, 880 (1997) (protecting indecent speech on the Internet even though the accessibility of the Internet makes access by children very likely to occur).

To the extent that Plaintiffs concern is motivated by a desire to preserve a certain level of obscurity, so that our faces and bodies cannot be instantly identified by virtue of a new technology, it fails to overcome two hurdles. First, this argument converts a descriptive account into a prescriptive one. The descriptive account is undeniable; it was once difficult to identify a person based only on her face or appearance while she was out in public unless you happened to know her. But the prescriptive account ("therefore we should be free from easy identification of our faces") is less convincing. Rather, it is an instantiation of status quo bias—an unjustifiable assumption that the amount of obscurity and exposure we are accustomed to *right now* is just the right amount.

Second, this status quo bias has no limiting principal and could have been applied to restrict technological advancements throughout history. The same arguments would have had emotional appeal at the advent of hand-held cameras, smart phone video recording, search engines, and social media.[4] BIPA has the purpose of blocking new forms of information as a precaution against speculative or unspecified harm, because "the full ramifications of biometric technology are not fully known." 740 ILL. COMP. STAT. § § 14–15(f) (2008); *See In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155, 1171 (N.D. Cal. 2016) (endorsing this purpose of BIPA). The First Amendment does not allow speech to be burdened for such a broad and abstract notion of privacy.

While there may indeed be uses of faceprints and facial recognition technology that can cause unjustified informational harm to society, it is premature to assume that the technology as a whole must be closely regulated, particularly since faceprints only augment what humans already do with their own eyesight and perception. The potential for misuse of an information technology cannot justify the restriction of *all* uses of that technology. Instead, a privacy statute must be designed to carefully minimize harmful information practices without unduly burdening other forms of speech.

To be sure, there may be some narrow contexts where the harms from identifying a previously unidentified person clearly outweigh the benefits. For example, restrictions on collecting any information (regardless of content) in front of healthcare facilities may also be compatible with the First Amendment. *See, e.g.*, *Hill v. Colorado*, 530 U.S. 703, 726–27 (2000).

[4] Banning the use of hand-held cameras because of privacy risks may seem absurd in the modern day, but it would not have seemed absurd to Samuel Warren and Louis Brandeis. The portable camera was the innovative technology that inspired their famous article, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890), and launched the legal recognition of a right to privacy. *See* Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 8 (1979).

Prohibitions on police use of facial recognition technology at assemblies and protests (or on police use of facial recognition more generally) could be legislated without implicating free speech protections if the bans apply only to state actors. Georgetown Amici Brief at 3; EFF Amicus Brief at 13. But a blanket prohibition on the creation of faceprints puts serious constraints on free expression without sufficient justification.

To the extent that BIPA protects privacy, those interests are outweighed by the burden on the rights of Clearview and others to create new information from publicly available photographs.

CONCLUSION

For the foregoing reasons, this Court should grant defendant's motion to dismiss consistent with the protections guaranteed by the First Amendment.

Dated: July 26, 2021

Amici Curiae First Amendment Clinic at Duke Law and Professors Eugene Volokh and Jane Bambauer

By: /s/ Rachel S. Morse
One of Their Attorneys

Rachel S. Morse
Cook County Firm No. 56232
MASSEY & GAIL LLP
50 East Washington Street
Suite 400
Chicago, Illinois 60602
(312) 283-1590
rmorse@masseygail.com